STATE OF MONTANA
DEPARTMENT OF CORRECTIONS
POLICY DIRECTIVE

Policy No. DOC 1.7.9	Subject: **ACCEPTABLE USE OF IT RESOURCES**
Chapter 1: ADMINISTRATION AND MANAGEMENT	Page 1 of 4
Section 9: Information Systems	Effective Date: Dec. 1, 1996
Signature: /s/ Mike Ferriter, Director	Revised: 04/26/07; 05/28/08

I. POLICY

Information Technology resources are under the exclusive ownership or control of the Department and may be used solely for the benefit of the agency. This policy provides guidelines to employees of acceptable uses and prohibited uses of the Department's IT resources.

II. APPLICABILITY

All divisions, facilities, or programs under Department jurisdiction or contract.

III. DEFINITIONS

Download – To copy software programs, games, screen savers and other such items from the Internet to a Department computer. Download does not include the copying of text documents from the Internet to a Department computer.

Employee – Any approved user of state IT resources.

Information Technology (IT) Resources – All computers, systems, software, utilities, peripherals and networks which are owned, provided, or controlled by the Department or the State including, but not limited to, e-mail, intranet, the Internet and SummitNet. As used in this policy, the term does not apply to telephones, cellular phones, or fax machines.

Internet – An electronic communications network that connects computer networks and organizational computer facilities around the world.

SummitNet – The State of Montana's telecommunications nucleus network or backbone connecting agency, university, grades K-12, library, and local government networks. SummitNet provides connectivity to the Internet.

IV. DEPARTMENT DIRECTIVES

Employees do not have a right of privacy in their use of IT resources. Agency system administrators, management, and Department of Administration personnel may monitor all aspects of employee usage of IT resources. Therefore, "Don't say, do, write, view, or acquire anything that you wouldn't be proud to have everyone in the world learn about if the electronic records are laid bare."

A. Acceptable Use of IT Resources

1. IT resources are used to conduct state business. Employees may be subject to restrictive or limited use of some IT resources, as determined by a supervising authority or administrator for business-related reasons.

2. IT resources may not be used for the employee's personal for-profit activities or non-profit organization of association activities that are not related to the employee's job duties. Employees may otherwise use IT resources as described in Section B.

3. In drafting and sending e-mail messages, employees should not include anything they are not prepared for the public to read. Statements can potentially become a basis for litigation, e.g., sexual harassment comments, and/or liability, e.g., statements contrary to the interests of the state government.

4. Employees will minimize unnecessary usage that may interfere with the effectiveness of the shared network and refrain from monopolizing systems, overloading networks with excessive data, or wasting computer time or other resources.

5. Employees will comply with all applicable local, state, and federal telecommunications and network regulations or policies, including, but not limited to, laws protecting copyright, commercial software, and intellectual property infringement.

B. Acceptable Personal Use of IT Resources

Employees may use state e-mail or the Internet for essential personal communications or information collection not otherwise expressly prohibited above. Such use must be kept to a minimum and not interfere with the conduct of state business.

C. Email Retention

Communications sent or received by the e-mail system may be documents under Article II, Section 9 of the Montana Constitution or public records under *Section 2-6-101, MCA,* and should be generated and maintained accordingly. Employees should delete items from their in-box and out-box when they are no longer needed. If a mail item needs to be retained, it should be moved to an off-line personal folder (on a network drive), an archive folder, or be printed. Items placed in an employee's archive are the employee's responsibility. The need for retention of an item should be reevaluated after it has been stored for 6 months. Employees can contact the state records manager with any questions on retention schedules.

D. No Right of Privacy in E-Mail Communications

Employees do not have a right of privacy in any IT resources. The Department or ITSD staff may periodically monitor, audit, and review e-mail and other IT resource transmissions at any time. Department of Administration personnel may also monitor e-mail.

E. Random Audits of Employee E-Mail

Employee email will be randomly audited on a monthly basis by division administrators or their designees.

F. Misuse of Email

E-mail is an extension of the workplace, and abusive or inappropriate e-mail will subject an employee to the Department's disciplinary policies, as outlined in *DOC Policy 1.3.1(A), Personnel Manual*. Employees may not transmit any sexually explicit images, messages, or cartoons. Department employees may not use e-mail for any communications containing

racial or ethnic slurs or epithets or anything that might be construed as harassment or offensive to others based on race, national origin, gender, sexual orientation, disability, or other classifications protected by state and federal law.

G. Downloading or Installing Software/Hardware

1. Employees may **not** install personal software/hardware from outside the office on Department computers, nor may employees bring their own computers or peripherals to the office to do Department work. This includes all personally owned data storage devices such as "pen" drives, CDs, DVDs, iPods and other portable media players, as well as personal digital assistants (PDAs), cell phones, and digital cameras. Employees who have a business need for specific data storage devices should request the device through their supervisor for review by IT staff.

2. Employees may not download or install software not specifically licensed to the Department and approved by the IBTB Manager through the Information Technology Purchase Request (ITPR) process. This includes all shareware, freeware and Beta release software products.

H. Portable, Laptop or Notebook Computers

Particular care must be taken by employees who use portable, laptop or notebook computers, including:

1. Locking a vehicle if the computer is inside of it.
2. Letting the computer warm to room temperature before starting it up after removing it from a vehicle during cold weather.
3. Not allowing unsupervised use of the computer while at home.
4. Scanning any diskettes used outside the office for viruses before using them.

I. Responsibility for Enforcement

Department supervisors and managers are responsible for ensuring that staff members follow the provisions of this policy in the use of Department computers. Employees will report violations of this policy to the appropriate Department authority.

J. Reporting and Disciplinary Action

Users will cooperate with system administrator requests for information about computing activities; follow agency procedures and guidelines in handling diskettes and external files in order to maintain a secure, virus-free computing environment; follow agency procedures and guidelines for backing up data and making sure that critical data is saved to an appropriate location; and honor the acceptable use policies of any non-state networks accessed. Users will report unacceptable use and other security violations to their immediate supervisor, to local personnel responsible for local network policy enforcement, or to personnel responsible for the security and enforcement of network policies where the violation originated.

If there is reasonable cause to suspect that an employee has violated this policy, the result may be immediate suspension of access to some or all IT resources pending further investigation. Confirmed violations will subject employees to disciplinary action up to and

including termination under *MOM 3-0130, Disciplinary Action,* and *DOC Policy 1.3.1(A), Personnel Manual*.

Supervisors are required to report all suspected violations of this policy, employee suspensions, resignations and terminations to the IT security officer as soon as the event takes place. The security officer will suspend the employee's accounts, thereby preserving evidence for investigation.

V. CLOSING

Questions concerning this policy should be directed to the Department's CIO or the IT Policy and Strategic Planning Officer.

VI. REFERENCES

A. 2-2-121, MCA (2007) Rules of Conduct for Public Officers and Public Employees; 2-6-101, MCA (2007) Definitions; 2-15-112, MCA (2007) Duties and Powers of Department Heads; 2-15-114, MCA (2007) Security Responsibilities of Departments for Data; 2-17-533, MCA (2007) Responsibilities; 18-4-313, MCA (2007) Contracts -- Terms, Extensions, and Time Limits; 45-6-311, MCA (2007) Unlawful Use of a Computer; 45-8-213, MCA (2007) Privacy in Communications; 53-1-203, MCA (2007) Powers and Duties of Department of Corrections

B. 2-17-504 through 528, MCA Montana Information Technology Act

C. Article II, Section 9; Montana Constitution

D. Volume 1, Chapters 1-0200.00 through 1-0250.30; and Chapters 1-1100.00 through 1-1110.00; Montana Operations Manual

E. 2-12-1 & 2; 2-13-101-107; Administrative Rules of Montana

F. ENT-INT-011, ENT-NET-031, ENT-NET-042; Enterprise IT Policy

VII. ATTACHMENTS

None.